Understanding the Design Space of Embodied Passwords based on Muscle Memory

Rosa van Koningsbruggen
Bauhaus-Universität Weimar
Germany
rosa.donna.van.koningsbruggen@uni-weimar.de

Bart Hengeveld
Eindhoven University of Technology
The Netherlands
b.j.hengeveld@tue.nl

Jason Alexander
University of Bath
United Kingdom
jma73@bath.ac.uk

ABSTRACT

Passwords have become a ubiquitous part of our everyday lives, needed for every web-service and system. However, it is challenging to create safe and diverse alphanumeric passwords, and to recall them, imposing a cognitive burden on the user. Through consecutive experiments, we explored the movement space, affordances and interaction, and memorability of a tangible, handheld, embodied password. In this context, we found that: (1) a movement space of 200 mm × 200 mm is preferred; (2) each context has a perceived level of safety, which—together with the affordances and link to familiarity—influences how the password is performed. Furthermore, the artefact's dimensions should be balanced within the design itself, with the user, and the context, but there is a trade-off between the perceived safety and ergonomics; and (3) the designed embodied passwords can be recalled for at least a week, with participants creating unique passwords which were reproduced consistently.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in interaction design**.

KEYWORDS

Embodied Interaction, Affordances, Movement, Explorative Research, Useable security, Authentication

ACM Reference Format:
Rosa van Koningsbruggen, Bart Hengeveld, and Jason Alexander. 2021. Understanding the Design Space of Embodied Passwords based on Muscle Memory. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3411764.3445773

1 INTRODUCTION

With the digitalisation of our world, passwords have become something which we encounter multiple times a day. Yet, passwords are not designed with usability in mind [1]. Common password restrictions, such as a minimum number of characters, not reusing a password, the requirement for special characters, uppercases, lowercases, and numbers, are designed to help people create safe passwords [18]. However, they also make it harder for people to recall their passwords, resulting in coping strategies including password managers, browsers that remember passwords, or less secure alternatives, such as reusing passwords or writing them down [23]. This has resulted in security processes, where the user is the weakest link in the system [40].

However, the main problem is not people's security-consciousness, but the heavy cognitive load that prevents them from generating safe passwords [3, 23]. Furthermore, password restrictions force people into behaviours which they perceive as too strict. This creates a conflict between their perception of how strong the password needs be and the enforced practise [1, 23]. To tackle this, password alternatives, such as biometric, graphical, haptic, and passwords which use muscle memory, have been developed (e.g. [4, 25, 26, 37]). Although the latter category shows promising results, the form, interaction, and scale of this type of password is as yet unknown. Therefore, this paper presents an exploration of the design space of tangible passwords which use muscle memory.

Based on the concepts of embodied interaction and muscle memory, this research aims to develop an embodied password which uses movement as the input modality. Using a Research through Design [50] approach, we conducted one exploration and five experiments. The process was explorative and iterative, where the results from each experiment were used to inform the next. The research started with an exploration of the movement space of passwords, followed by experiments regarding the affordances and interaction. In these experiments we examine how gestural input affordances influence our perception of safety, the design of embodied passwords, the role of dimensions, as well as the contexts in which passwords are used. Furthermore, we investigate the memorability aspects of embodied passwords, by exploring how people compose and recall them.

The overall contribution of this research is an understanding of the fundamental aspects of embodied passwords which use muscle memory. Specifically, the research gives an indication of the suitable movement space, how to elicit those movements via an artefact, the role of the dimensions of the artefact, and lastly, the variety and memorability of embodied passwords. Before discussing the exploration and experiments which have resulted in these insights, this paper will first discuss the theoretical background concerning embodiment, affordances, muscle memory, and alternative passwords.

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445773

2 THEORETICAL BACKGROUND

2.1 Embodied Interaction and Movement

Although closely aligned to tangible interaction [22], embodied interaction focuses on how the human body can be used to directly manipulate an artefact's body, as such creating meaning *in interaction* [42]. Instead of using tokens and constraints, embodied interaction focusses on using the artefact's body as the source that controls the Graphical User Interface (GUI). For example, one can squeeze or flip the artefact in order to perform an action [11]. The interaction with the object is what allows the user to create meaning. As explained by Dourish, embodied interaction focusses on the creation, manipulation, and sharing of meaning through our interactions with objects [10]. Although embodied interaction is more than capitalising on our bodily skills and familiarity with objects [10], these elements can reduce the cognitive load sometimes associated with traditional GUI interactions [42]. Furthermore, a crucial element of embodied interaction is movement: *"embodied interaction refers to the ability to involve one's physical body in interaction with technology in a natural way, such as by gestures"* [32]. Movement forms the start, foundation, and premise for our way of being in the world [14]. However, despite this, the role of our actual human body is often overlooked in the design and writing of embodied interaction. Limiting a meaningful, interesting, and aesthetic fit among movement, action, and interaction [21]. Therefore, we explore whether embodied interaction could be used for a password using a soma design approach [21].

2.2 Affordances

As described by Gibson, people (and other animals) are able to perceive what action possibilities their surroundings have to offer them [16]. For example, a couch offers the affordance of sitting to a grown person. However, it might offer another affordance to a toddler who is just learning how to walk. The toddler might use the couch as a bar to obtain balance. As such, an affordance represents the relation between our bodies and the world, and depends on the actor's own capabilities [16].

Designing for affordances is especially interesting for interactive products. By including computation, new action possibilities can be created. For example, shape changing interfaces, where the shape of an object can adapt itself to new contexts [24], as such increasing their usability [2]. Or action possibilities that only appear once a previous action has been performed, also called sequential or nested affordances [15]. Quite commonly, affordances only focus on our cognitive skills, however they can also focus on other senses such as touch or sound [15, 19]. It is based on the designer's understanding of affordances, that the interactions can either be easy or hard to perform.

One of the aims of this research is to explore how certain movement qualities can be elicited by objects, how an object can facilitate a feeling of security, and what the link between object and environment is, hence exploring the affordances of an embodied password.

2.3 Muscle Memory

We all perform actions which have become extremely familiar, but once took effort to learn. Repetitive physical actions such as cycling, walking, swimming, knitting, etc., all become part of something which is referred to as muscle memory [30]. Muscle memory is a type of implicit memory, which is associated with two brain areas: one part which exerts control over the learning of action sequences, so that even the most complex set of actions can become automated (this is called 'habit learning'), and a part that uses messages to finetune the actions [30]. When learning a new action, such as writing, the habit learning brain part groups together the individual motor elements and forms an action sequence. This action sequence is then performed with decreasing variation; each time the action becomes slightly better, faster, and more precise. This happens with the guidance of the brain part that is responsible for adaption and fine-tuning movements. Through time, these learned action sequences can even become so hard-wired, that they become similar to innate behaviours: behaviours which are a result of our genetic memory, such as breathing [30]. Furthermore, they can easily be recalled without conscious effort, even when they have been unused for months [41, 44].

These qualities have not gone unnoticed by Human Computer Interaction (HCI) researchers, who have used muscle memory for a variety of purposes, such as helping people with eyes-free typing [33], as an integral part of kinaesthetic interaction [13], and for passwords [35, 37]. Because of the hardwiredness and its potential for a password alternative, one of our aims is to further explore how muscle memory can be used for an embodied password.

2.4 Alternative Password Approaches

Lastly, we will discuss some alternative password approaches; some of which are already (commonly) used, such as biometric passwords and graphical passwords, and some which present first examples, such as the TangibleRubik [37] and Bend Passes [35].

There is an increasing use of biometric passwords, where authentication happens automatically, based on a person's physiological or behavioural characteristics [25]. These passwords rely on who you are and what you do, as opposed to what you have (such as a passport) or what you know [38]. Biometric passwords are highly personal and effective, but can pose limitations as well. For example, how would you reset your password in case you got hacked? You cannot change your own DNA or adopt a new behaviour. Also, and perhaps more relevant, do we trust companies with such personal information?

Pitched as a solution for the memory burden of alphanumerical passwords [17], graphical passwords can take numerous forms. An example is the pattern lock as used on Android phones, which give the user the freedom to swipe their own line drawing across a small matrix. Other examples ask the user to select particular areas of a picture [49] or ask them to make a doodle [17]. Despite the variety, all rely on the human ability to remember images or visual patterns better than text [43]. Although graphical passwords are already a step towards accepting unique inputs that suit their user, they are prone to smudge attacks [35], and limit us to 2D interfaces and our finger(s).

Lastly, there are examples of tangible passwords which use movement. A first example is TangibleRubik [37], a tangible password which explored whether motor learning capabilities could be used

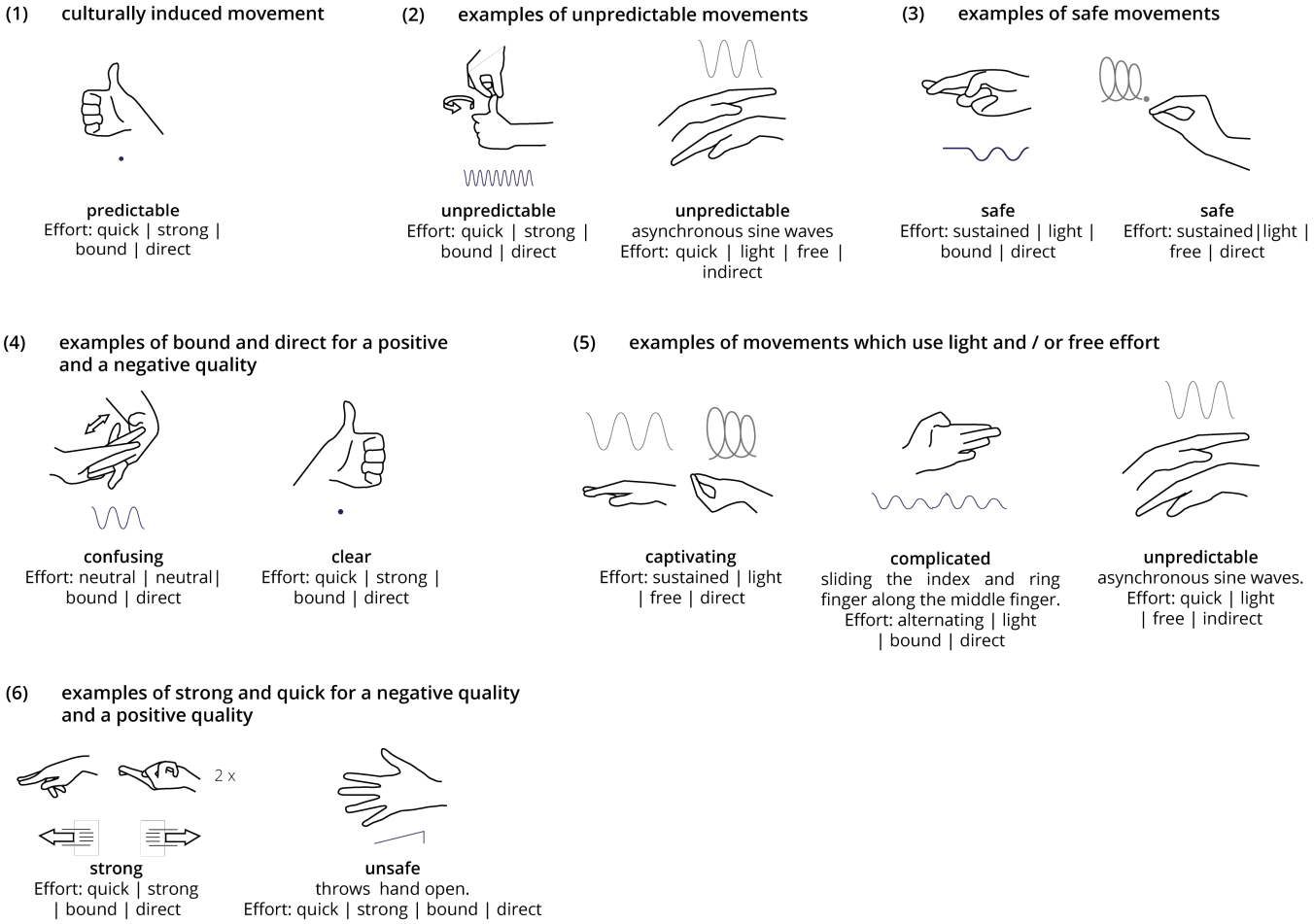

Figure 1: A visual overview of the results mentioned in section 4.1.1. The pictograms represent the movements created by the music conductor(s) (students). The lines and arrows indicate the direction of the movements. Whenever there is a dot beneath a pictogram -see "predictable" and "clear"- it indicates a static movement. Straight lines, such as with "unsafe", indicate abrupt movements, whereas waves indicate flow.

for passwords. Here, people can manipulate a Rubik's Cube in order to log in, where the combination of movements represents the user's password. In a lab study this research showed that the participants could recall a password based on motor skills after a short interruption. A second example are Bend Passes [35]. Here bend gestures performed on a flexible interface represent the user's password. Bend Passes explored the creation, the memorability, and the security of Bend Passes, both created by the users themselves and assigned. The research shows that 81% of the participants were able to recall the self-created Bend Passwords for one week and 63% recalled their assigned passwords. Furthermore, this research provides first insights in how people recall and compose their bend passwords [35].

Although these examples indicate that people can recall passwords which use muscle memory, and Bend Passes already provides insights in how people compose and come up with this type of password, they do not provide insights into the interaction, affordances, and design of muscle memory-based passwords. TangibleRubik is a proof of concept, leaving the design of the artefact out of its scope, and the design of BendPasses are heavily based on the technology. Therefore, we use a soma design approach [21] to explore what the interaction with muscle memory-based passwords should be and how to facilitate this interaction through the design of an embodied password artefact. The aim of this research is to offer guidelines for future embodied passwords based on muscle memory.

3 METHOD

The overarching goal of our research is to explore whether embodied passwords based on muscle memory can be used as an alternative to alphanumeric passwords. In order to do so, we need an understanding of whether people are able to use and recall embodied passwords. However, before we can study people's ability to recall and use embodied passwords, we need to understand the characteristics of an embodied password: what movements, shapes, interactions, and dimensions make sense for an embodied password?

In order to explore these elements, we conducted one exploration and five experiments. The exploration and the first experiment focus on understanding which movements are suitable for passwords and the dimensions in which these need to be performed. The findings were then used to design an artefact which elicits these movements and explore the interaction of an embodied password. Lastly, we explored the role of the dimensions of the artefact and tested the memorability of the designed embodied password.

The experiments will be discussed in three overarching themes: (1) the movement space, (2) affordances and the interaction, and (3) the memorability. The role of dimensions and the memorability experiment will be discussed in-depth. For brevity, a summary of the main findings will be given of the exploration and the other experiments.

4 THE MOVEMENT SPACE

The first step towards an embodied password was to gain an understanding of the movements suitable for a password and the dimensions in which these movements need to be performed. In this section, we will discuss the setup and the results.

4.1 Expressivity of Movements

The aim of the first exploration was to gain initial insights in movements which are suitable for a password and which are not. For this experiment, four music conductors and two music conductor students were asked to express password qualities with their hands. The experiment focussed on music conductors, as they are trained to use their hands to convey emotions or messages. The qualities asked were both positive (such as safe) and negative password qualities (such as unsafe), in order to create an overview of the type of movements to design for and which to stay away from. Except for "safe" and "unsafe", the qualities came from the AttrakDiff questionnaire [20], in order to use terms which have been validated. Terms were filtered down to those that could potentially fit an embodied password. With the consent of the participants, the hand movements were filmed and analysed using the Interaction Quality Framework [39]. One of the music conductors was asked to take part in an interview, to get an understanding of the movement principles behind conducting.

4.1.1 Results.

From the analysis it seems that some qualities elicit a similar or culturally induced movement, as can be seen in figure 1 under 1. For example, the qualities "simple", "clear", and "predictable" often triggered the user to make a "thumbs up" sign. Other qualities, such as "unpredictable", resulted in a variety of movements, a complexity in direction, and focussed on small gestures, see 2 for examples. Interestingly, movements which were associated with "safe" were light and direct in their effort, as seen under 3. Overall, the movements created for both the positive and negative qualities were bound and direct in effort (see 4), meaning that the movements were controlled, careful, constrained, and single-focussed, laser-like [39]. The positive password qualities mainly focussed on quick and strong movements, although sometimes light and free movements were created as well. The light and free movements, as seen under 5, were composed for qualities such as "complicated", "unpredictable", and "captivating". Furthermore, the gestures created for the positive password qualities were longer and showed more effort variation. Whenever a negative password quality scored the effort elements strong and quick, it was because the gesture was short and performed with force. On the contrary, for the positive password qualities it meant a long movement performed at a high speed, see 6. A summary of these findings with exemplary movement pictograms can be seen in figure 1. All pictograms and video footage of the movements can be found in the additional material.

From this exploration it seems that a movement suitable for a password should focus on a quick, strong, bound, and direct effort. However, users should have the freedom to alternate with free and light effort qualities, in order to create unpredictable and captivating passwords.

4.2 The Spatiality

Although the previous exploration gave insights in the effort qualities of password movements, it remained unclear within which dimensions, or spatiality, these movements should be performed. Some gestures used a lot of space, whereas others solely focused on finger movements. Therefore, we setup an experiment to explore the spatiality of an embodied password.

During this experiment participants were asked to create a password using hand movements within four boxes with different dimensions (see figure 2). The dimensions of the four boxes were based on the gestures made in the exploration, with the biggest box being large enough to facilitate the largest gestures and the smallest being large enough for the smallest gestures. Eighteen participants took part in the study (of which eight identified as female and an average age of 22.3 years), all design students.

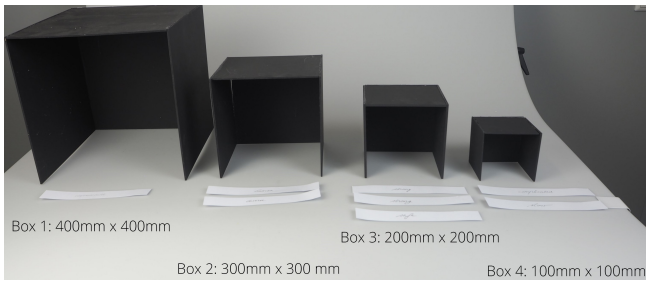

Figure 2: The setup of the experiment. Cards containing the positive password qualities have been assigned to the different spatialities.

At the start of the experiment, the four boxes were placed in front of the participant, together with cards containing the positive password qualities from the previous experiment. Participants were asked to put their hand in the boxes, imagine that they had to make a movement within the box which would function as their password, and assign the qualities to the spaces. If a quality could not be assigned or if the participants believed it belonged to multiple spaces, that was fine as well. The walls of the boxes were covered, in order to prevent the participants feeling watched or judged.

In order to analyse which spatiality was most desirable, the number of times a quality was assigned to a box was recorded, together with the number of times a quality could not be placed.

Furthermore, participants were asked to mention why they assigned a quality to a box.

4.2.1 Results.
During this experiment the biggest box was most often referred to as unpredictable. Moreover, due to the large space there was no need to be cautious: *P2: "you don't need to be cautious within this space"*. On the contrary, the smallest box was regarded as complicated, since it was hard to create a movement within the minimal space. When looking at which box the participants preferred, box 3 was the most common, as it fitted the participants' proportions best and allowed them to create both large and fine movements: *P8: "This space is just big enough for my hand proportion and gives me enough room for very fine movements and still some bigger movements as well."* Participants also stated that box 3 offered a sense of safety, since the relatively small space gave the feeling that nobody could see their movements: *P14: "It is such a small space that nobody can see what I am doing."* Interestingly, the participants mentioned that they were inclined to make slow and cautious movements in the smaller boxes, whereas the bigger boxes invited stronger and faster movements. Based on these insights we decided to use the dimensions of box 3 for our further research.

5 AFFORDANCES AND INTERACTION

The findings of the exploration and the first experiment give an indication that the movement space of an embodied password should be around 200 mm x 200 mm (relating this to an average hand [9] means slightly longer than a stretched hand and around 2.5 times as wide as a hand). Furthermore, the movements of the password should have the effort qualities of being quick, strong, bound, and direct, but offering the user the freedom to alternate with free and light. This way, the user can create unpredictable and captivating passwords.

Having gained insights towards the movement space of an embodied password, the next step was to explore potential password input artefacts. In this section, three experiments will be discussed to varying extent, focussing on the shape, the interaction, the environment, and the dimensions of an embodied password.

5.1 Making it Physical

With an idea of the type of movements, effort, and spatiality suited for an embodied password, the question arose how to elicit these through a password input artefact. Therefore, we conducted a pilot study to explore whether these movements, effort qualities, and spatiality could be elicited with physical artefacts, in order to create an embodied password. Based on the video analysis of the first exploration, twenty device mock-ups were designed, evaluated, and reduced to eleven artefacts, which can be seen in figure 3.

This selection was then used in a mapping experiment, to explore whether the design could be related back to the original gestures and to check whether the translation between gesture and artefact was performed successfully. Ten participants took part in this experiment. At the start, they were shown video footage of the gestures and received cards with the gesture pictorials (see figure 1 for pictorial examples), plus the device mock-ups. The video footage could be replayed and the cards were laid down in corresponding order to the footage. Next, participants were asked to assign the pictorials to the device mock-ups and explain why they assigned them as such. Participants were allowed to play with the mock-ups themselves and could assign multiple gestures to one mock-up, or vice versa.

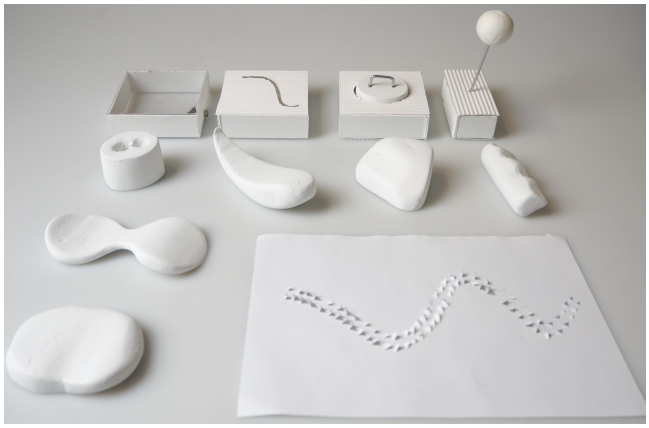

Figure 3: Overview of the created mock-ups which would facilitate the gestures created by the music conductors and music conductor students.

From this pilot, we saw that three mock-ups could be best related to the original movements and had the clearest design according to participants. These mock-ups can be seen in figure 4. The "wave" was linked correctly eight times, the "joystick" seven, and the "twist" six. Interestingly, the wave is a static object, whereas the others facilitate a more active interaction with the artefact itself. These mock-ups could be used as password entry devices.

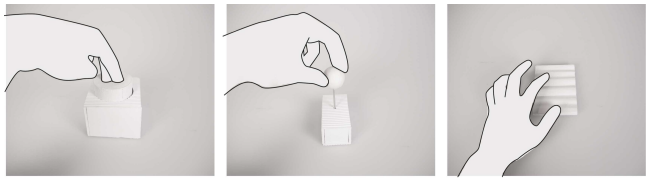

Figure 4: Images and interaction with the three mock-ups.

5.2 Usage and Context

The three artefacts from the previous pilot study were then used in our next experiment, with the aim to explore how people would use them to create a password and in which context(s). For this experiment participants had to walk through four scenarios in which they had to unlock an item: ATM, laptop, mobile phone, and a door. Within these scenarios, participants were asked to enter a PIN-code, passwords for their laptop and mobile phone, and to unlock a door, using the three artefacts. Furthermore, they were asked to explain the design decisions behind their password and which artefact they would choose for the experienced scenario. With the participants' consent, all movements and interviews were recorded, in order to analyse how the artefacts were used and to make transcripts. The video transcripts were analysed using open

coding and the audio transcripts were analysed using thematic analysis [7]. In total, twelve participants took part, of which six identified as female, an average age of 24.4 years, all design or HCI students.

5.2.1 Results.
A summary of the results follows. The (thematic) analysis of the recordings resulted in three clusters of quotes and accompanying movement qualities:

(1) Perceived necessary safety, meaning that the different password applications required a different level of perceived safety. For example, for the mobile phone, passwords were quick and short, whereas for the ATM, passwords were much slower and composed, something participants did not mind: *P2: "It does not need to be fast. [...] it should be precise, I believe. And very unique!"*;
(2) Familiarity, meaning that participants automatically associated some of the shapes with specific contexts or vice versa: *P10: "Well, the first thing I think about when I see this [the ATM] is that I associate it with numbers, and this [the laptop] with that ridiculously long organisational password, and this [the phone], for this I have a vague swiping password."*, which influenced the created passwords. To illustrate: for the mobile phone participants created swipe-like motions, a movement commonly performed on a phone; and
(3) Design feedback, meaning that participants wanted the artefact to include two things. First, the artefact should communicate its current state. For example, whether the device is already unlocked, or a door handle which would become visible once the password is entered correctly. Secondly, the password artefact should account for rhythm, speed, and acceleration: *P4: "Perhaps something with a speed authentication."* These elements could be useful to incorporate in future embodied password designs.

Of the three artefacts, the rotary interface "the twist" (see figure 4), was preferred in three of the four scenarios (ATM, laptop, door). The passwords created with this interface were seen as safe, it provided a wide variety of movements, and offered affordances for a clear start and end of the password, as participants lifted the cylinder to indicate the start of their password and pressed it down to complete it. This is an important movement element according to the music conductors of the first exploration. Therefore, the decision was made to use the twist as the basic shape and interaction for further exploration. In order to do so, a next iteration of the artefact was designed, as seen in figure 5.

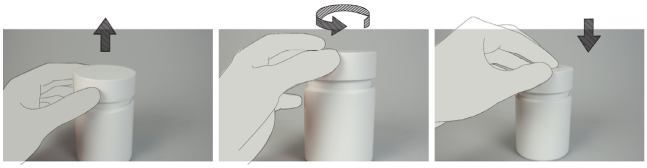

Figure 5: The embodied password interface. To start the password you lift the top part, after which you can start rotating. In order to enter the password, the top part is pushed back in.

5.3 Specifying Dimensions and Increasing Realism

Having found the basic artefact form, we set out to determine the most appropriate dimensions for the artefact. We created a 3 × 3 grid of the same artefact with alternating dimensions, as shown in figure 6. Along the x-axis, the diameter of the interface changes with a factor of two and along the y-axis the height of the cap changes with a factor of two. This factor was chosen to ensure that the smallest cap nicely fits between one's fingers and the biggest cap just fits a stretched average hand, keeping the relation to the human body.

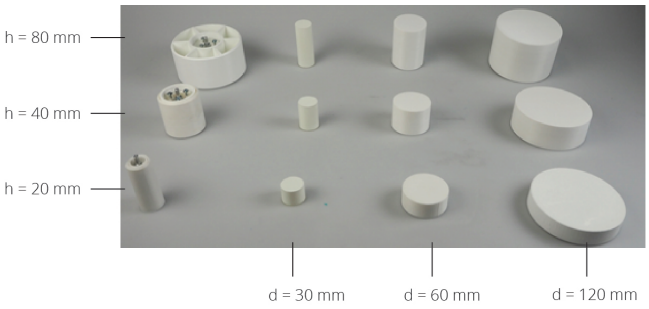

Figure 6: Dimension-grid of the interface caps (right, 3x3 matrix) which are attached to the hardware housings on the left. The height of the housing stayed constant (40 mm). H indicates the cap-height and D the diameter of the artefact.

To increase realism we decided to start the experiment with a priming session, to create an alert feeling which people normally experience when entering a PIN at an ATM. In order to do so, participants were shown a movie clip at the start of the experiment. We used two clips from a set selected by a Film and Literature Studies student. The initial set of suggested clips was tested with nine participants, to assess how much negative valence they generated using the PANAS-questionnaire [47]. We followed a similar setup as [48, p. 117-125]. The two clips with the highest average negative valence scores (26.4 and 26.6) were then used during the experiment.

For the experiment, sixteen participants— of which six identified as female, an average age of 27.6, thirteen HCI-students, one manager, and two HCI-teachers—were twice given three objects to use as a password input device and assigned to one of the four scenarios used in the previous experiment. At the start, participants were shown the first movie clip, after which they had to create three passwords with their initial set of artefacts. Having created the passwords, participants were asked which artefact from the set they preferred and why. After this, participants were shown the second movie clip, and the process repeated itself with a new set of artefacts. The passwords and interviews were recorded with the participants' consent. The video footage was analysed through open coding, and the interviews were transcribed and analysed using thematic analysis [7].

5.3.1 Results.
In general, participants preferred two artefacts: the smallest, with a

diameter of 30 mm and a cap-height of 20 mm, and the middle-sized, with a diameter of 60 mm and a cap-height of 40 mm. The smallest artefact was considered the safest and leaving you in control. Participants who preferred the middle-sized object made a trade-off between the perceived safety of the artefact and how ergonomically pleasing it was: *P8: "[I prefer] size 1 or size 2, because size 2 is nicer to hold, but size 1 is probably safer."* Moreover, participants stated that the artefact's dimensions should be balanced within the artefact itself, with their bodies, and with the context: *P2: "That's why I turned it [the biggest object], because it felt out of balance."* and *P9: "I would like either the smallest or the biggest. The smallest fits nicely within my fingers and the biggest in my hand."* and *P14: "The largest is just too large for a door."* Lastly, participants mentioned that the artefact should be concealable.

6 MEMORABILITY

The final aim of this research was to explore the memorability aspects of the embodied passwords. After all, one of our starting points was to capitalize on people's muscle memory. In order to do so, we decided to make fully working prototypes of the two preferred interfaces of the previous experiment (see figure 7), and set up a final experiment.

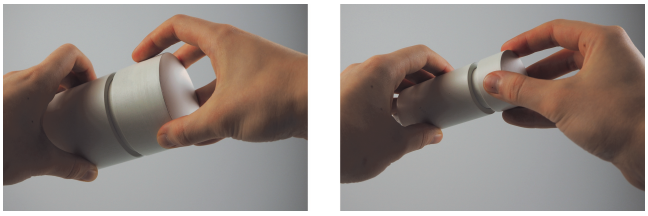

Figure 7: The artefacts used for the memorability experiment.

The working models were created using the Sprakfun ProMicro and an 8-bit absolute encoder (in our case [6]), within the Arduino environment. By rotating the cap, the encoder registers the direction of the movement and its position. By either changing direction or holding the same position for one second, the user can indicate that a "movement" has been performed. The selected positions are then saved in an array, resulting in a codified version of the embodied password, which is used to verify whether the password is entered correctly. Since it is nearly impossible to perfectly replicate the initial movements, an error margin was added. The error margin depends on the size of the movement: the bigger the movement, the larger the allowed error margin, as it is harder to precisely reproduce large movements with the prototypes. The maximum allowed error margin was twenty steps above or below the original value, and the smallest margin five steps above or below. The error margin is calculated by checking whether the ratios of the movements were the same or if the number of steps equalled the original movement. Only if all movements of the embodied password fall within the error margins, the password is entered. To increase realism, the prototypes were connected to a pre-programmed web-interface of a fictional bank. By successfully entering an embodied or alphanumeric password, the user would unlock the bank account.

The experiment itself consisted of three sessions. In the first session, participants (see table 1) were asked to fill out the VAK-questionnaire [8], to get an understanding of their preferred learning style and to see whether this influences how well a certain type of password is recalled. Next, participants were asked to create embodied passwords with the prototypes and two alphanumeric passwords (meant as a baseline) for a fictional bank account. This setup was inspired by [17] and [35]. The alphanumeric password had to comply to the password restrictions commonly used by banks (at least eight characters, including a number, special sign, and capital letter). Furthermore, the passwords should not have been used before, nor contain personal information. The restrictions for the embodied passwords were that the password should have a minimum length of three movements, of which at least one varied in size or direction. The difference in restrictions was purposeful, as it is yet unknown whether people can recall the embodied password, but it is known that people can recall alphanumeric passwords.

Participants first created the alphanumeric passwords. Each password had to be entered correctly twice to verify it, as commonly required by online services. Next, participants had to create their embodied passwords. Starting with the smallest artefact, participants were shown an example of how the interface worked, after which they could familiarise themselves with the prototype. Based on a pilot study, the decision was made to let the participants practise their embodied password five times (inspired by the research setup of [36]) with a visual notation map of their password, as can be seen in figure 8. The visual notation maps [31] of the movements were automatically drawn in Processing. These maps served three purposes: to create a visual overview of the passwords, to see how accurately the passwords were reproduced, and as a hint for when a participant had forgotten their password. For each password, participants were allowed three attempts. If a participant could not recall their password within this limit, they were shown a hint of their password, to see whether this would help them recall. The number of attempts required and whether a hint had to be given was recorded. If the hint still resulted in a failed attempt, a new password had to be created.

After the familiarisation rounds, the embodied password had to be entered correctly twice without the visual feedback, in order to verify it. This process was repeated with the biggest prototype. After this, the participants were asked how they had designed their embodied passwords, how they experienced them, and how they felt using them.

The following day, participants were asked to return for the second session, where they had to re-enter their passwords. The third session took place a week after creating the passwords. This session started with re-entering the passwords, after which a semi-structured interview took place. The interview focused on how the participants experienced the embodied passwords, how they recalled them, what they believed the strengths and weaknesses of the embodied passwords were compared to alphanumerical passwords, how they had created and recalled their alphanumerical passwords, which interface and which type of password they preferred, and lastly, what they would change or add to the interfaces.

Fourteen participants took part in this experiment, see table 1. The questions asked at the end of the first session and the semi-structured interview were recorded, transcribed, and analysed using

Table 1: An overview of the participants' demographics

Average age	29.8 years
Standard deviation	12.1
Gender	8 male
	6 female
Preferred learning style	5 Kinaesthetic
	5 Visual
	4 Auditory
Occupation	7 HCI PhD students
	5 Design Masters' students
	1 Teacher
	1 HCI Manager

Table 2: The average attempts required to successfully enter the password

Average needed attempt	Session 2	Session 3
Embodied password	1.4 attempts	1.1 attempts
Alphanumeric password	1.2 attempts	1.5 attempt

thematic analysis [7]. Moreover, the password movements were videotaped during the first session, to review the grip and movement.

6.1 Results

One of the aims of this experiment was to explore whether people could recall and reproduce embodied passwords. During the second session, two participants forgot one embodied password, but recalled them after being shown the notation map. Further, one participant forgot one of the alphanumeric passwords and could not recall it after the hint. Therefore, a new alphanumeric password had to be created.

During the last session, all participants could recall and reproduce their embodied passwords. One participant forgot all alphanumeric passwords and another participant forgot one of the alphanumeric passwords. Both could not recall the passwords after being shown the hints. Based on this, it seems that people are able to recall embodied passwords and that the preferred learning style does not influence their ability to recall a certain type of password. Moreover, the average number of times needed for a successful entry was calculated, which can be seen in table 2.

6.2 Thematic Analysis of the Interview Data

Our thematic analysis resulted in insights about the strengths and weaknesses of embodied passwords, as well as insights about the design and the interaction. In this section the highlights will be discussed. Before each quote, the session number can be seen, which is either session 1 (*S1*) or 3 (*S3*). The participant number is given by *P*.

6.2.1 *General Strengths and Concerns.*

Strengths of the embodied password were that they were easy to recall and the interaction was seen as personal, intimate, playful, and unique to you: *S3P6: "The advantage is the intimacy. Only you can feel your hands."* and *S3P13: "I really like that it is very personal. I believe that, especially when the movement is a bit more complex, people cannot copy it, because they are not you."* Although the embodied passwords were experienced positively, nine participants believed that the embodied passwords were not secure for three reasons:

(1) **Visibility**: Eight participants mentioned that they were concerned with the visibility of the password: *S3P1: "I do not know about the safety.[…] maybe if you make sure that nobody is watching you, then maybe it is safe."* However, others stated that they did not believe this was a valid reason, as people can also see what you are typing: *S3P12: "I am not sure about other people seeing you doing it, but on the other hand […]. If someone looks at what you are typing, it is not that hard to figure out."* This made participants wonder what created this feeling, bringing us to the second reason:
(2) **The password felt easy to enter and easy to recall**: Participants stated that the embodied passwords were easy to recall, as they felt logical and natural to them. This made them wonder whether this would be the same for others: *S3P9: "I do not know whether it is easy to guess for others. To me it feels really easy."* and *S3P3: "If you are reasonably able to reproduce it without much cognitive effort, then what are the implications of that with another person?"* It seems that a password needs to feel or be complex in order to be perceived as secure: *S1P13: "The first one felt really safe, as it was very complicated."*
(3) **The uniqueness of the created movement**s: Lastly, four participants wondered how unique their movements were compared to others: *S3P4: "How typical are those passwords? Because perhaps the rotation that is natural to me, is natural to other people as well."*

Besides these security concerns, one participant mentioned that at the moment it would be difficult to have multiple embodied passwords: *S3P12: "If you have ten passwords like this, then you have a problem, because you can't really have something like a context with it."* Furthermore, the embodied passwords did not give an indication whether you were entering the correct password or whether what you had done was correct: *S3P10: "Did I do something wrong? I don't think so. Did I enter the wrong password? I don't think so. So there is this feedback problem."*

6.2.2 *Composing Embodied Passwords.*

We discerned four distinct strategies to compose an embodied password: (1) The first was to create movements of which the feeling could be recalled: *S1P7: "I started uncomfortable and ended uncomfortable, so I know how it feels."* (2) A second strategy was to create passwords based on a beat or a song: *S1P2: "In my head I created like a musical thing."* (3) Thirdly, participants created certain rules for themselves: *S1P9: "The bigger one was for the savings account, which is long term, so that is why the final movement was a big rotation."* (4) Fourthly, two participants created embodied passwords based on alphanumeric passwords.

Interestingly, three participants created an embodied password based on what felt natural to them without any strategy. The participants could all recall these passwords, although one participant had to be shown a hint.

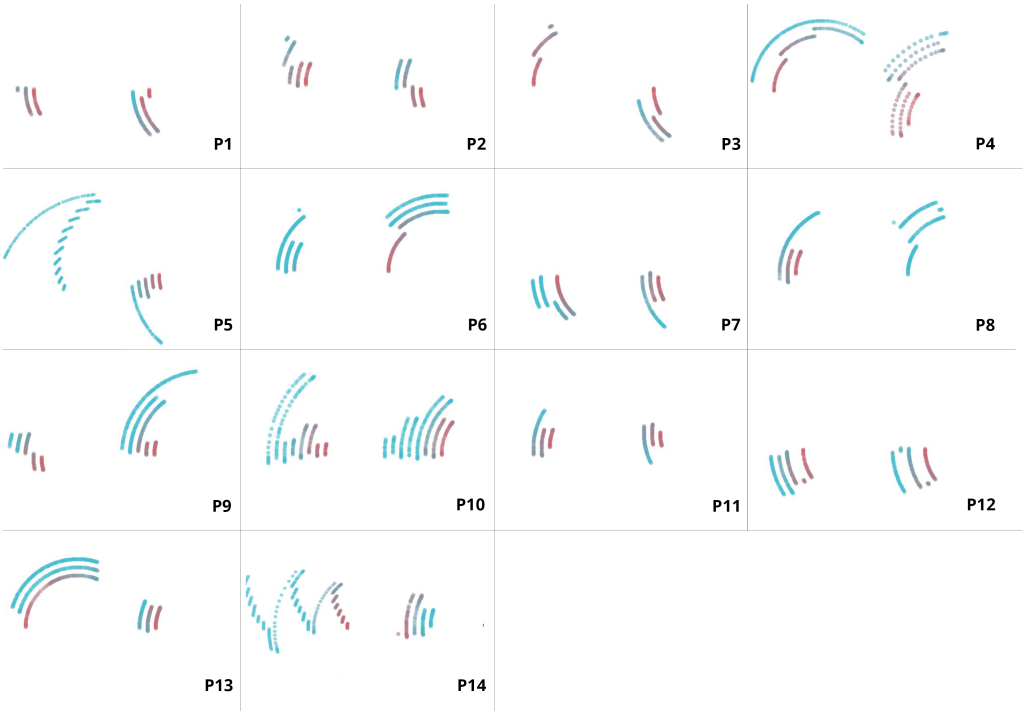

Figure 8: Overview of the notation maps. The notation map on the left shows the password for the smallest prototype and the map on the right for the biggest. The participant number is indicated with *P*.

Figure 8 shows an overview of all the embodied passwords. As can be seen, no password was identical. Although 36% of the embodied passwords focussed on the minimal required length of three, some participants created passwords which were considerably longer, consisting of more than ten moves (see P5 and P14). However, most participants stayed within one "movement range". The given reason for this was the natural boundary of your hand and wrist. The percentage of minimum length was 7% for the alphanumeric passwords,with most passwords having a length of 9-11 characters and none longer than 19. Looking at the passwords, there does not seem to be a direct link between the dimensions of the artefact and the created passwords.

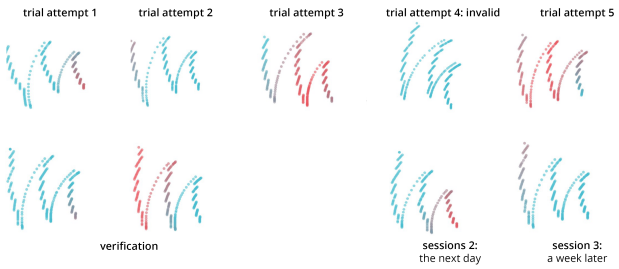

Figure 9: Participant 14's embodied password, of 21 moves, throughout the experiment. Trial attempt 4 was invalid, meaning that the password did not match the original.

Besides the overview of all the created passwords, an overview of how the passwords evolved was made. An example can be seen in figure 9. As mentioned earlier, to enter the password, the movements had to be the same ratio and/or hit the same values as the initially selected password. Slight deviation was allowed according to the programmed error margin. Throughout the sessions participants were able to consistently reproduce their passwords. An example can be seen in figure 9, which—despite focussing on one of the longest passwords— shows a consistency throughout the experiment. The notation maps show a high similarity, with the exception of trial attempt 4. This attempt deviated too much and resulted in an invalid entry. The complete overview, together with footage of the movements, can be found in the additional material.

6.2.3 *Recalling Embodied Passwords.*

The embodied passwords were seen as easier and faster to recall: *S3P5: "For me it is easier to remember a movement [...] because it has always a reason."* and *S3P12: "Somehow the movements felt familiar, as if I had done this my entire life."* Besides, participants mentioned that having a strategy helped with recalling: *S3P6: "I remember the strategy that I explained so then I knew that. [...] It made me feel like less constrained in remembering them and less anxious that 'oh you are not going to remember it'. In some way it was more organic."* Interestingly, some participants only recalled their passwords once they had to enter them: *S3P7: "But I didn't remember the exact sequence and so on. Until I did it, basically."*

6.2.4 *Feedback on the Embodied Password.*

Twelve participants mentioned that they wanted some feedback

with their embodied password. This feedback should provide guidance when replicating the password, as such providing some reassurance of reproducibility, and communicate whether the created password is a "good" password, or whether the entry was successful. Haptic feedback was mentioned the most, as it is discreet and subtle: *S3P5: "It would be cool to have some kind of resistance, so some kind of haptic feedback maybe. Something that is not very obvious, really subtle"*. Visual and audio feedback were mentioned as well.

Another element of improvement were sequential affordances [15] that would allow you to only start entering your password once the device is prompted: *S3P7: "this one opens up when it is time to type the password kind of thing. So you know as the user that it is connected. It is time to do it."* An element which was seen as positive by the participants was the clean and minimal design: *S3P12: "I like that they are white. They are really clean and inspire you. Like a blank sheet, you can do whatever you want."*

7 DESIGN IMPLICATIONS

In this section we briefly present design implications for embodied passwords based on muscle memory derived from the findings of our studies. The exploration and first experiment have given us an idea of the movement space of passwords. Password movements should have a quick, strong, bound, and direct effort, with the freedom to alternate with light and free. This way, the user can create unpredictable and captivating passwords. The movements should be performed in a spatiality of 200 × 200 mm. Translating this to ratios, the spatiality should be slightly longer than the average stretched hand and around 2.5 times the width [9].

Regarding the affordances and interaction, we have found that a cylindric shape worked well for the creation of a variety of "safe" passwords with a clear start and end. The context of a password has a perceived necessary safety, which together with the affordances and link to familiarity, influences the passwords people create and how they are performed. Moreover, the dimensions of the artefact play an important role in how people perceive and use it. Smaller dimensions are seen as safer, however, in our research we found that there was a trade-off between the perceived safety of the artefact and how ergonomically pleasing it was. Furthermore, the dimensions of the artefact should be balanced within the design itself, with the user, and with the context.

Lastly, this research has shown that people can recall embodied passwords for at least a week. In our memory experiment, participants all created unique passwords, using different strategies. However, participants had concerns regarding the visibility of the passwords, the fact that they felt easy to perform and recall, and the uniqueness of their movements. A main point for improvement would be feedback, which should provide guidance and a way to communicate with the user.

8 DISCUSSION

This research has generated insights in what an embodied password could be, what the interaction should be, and the memorability aspects of embodied passwords. The presented findings can be used for the design of future embodied passwords, password alternatives, or objects which could make the user feel safe. In this section we briefly discuss our main findings.

8.1 The Influence of Dimensions and Movement

For the design of embodied passwords, it is important to consider how the dimensions of the password artefact influence the perceived safety of the object. In this research, the smaller objects were seen as safer and more comfortable than the larger sized equivalents. This might be because the larger objects were harder to cover with your body, hence more visible. However, it could also stem from the feeling of control. With the smaller objects, participants felt as if they were the ones in control, whereas with the bigger objects, it felt as if the object controlled them.

The feeling of "small being safe" can be observed in the movement qualities of the passwords as well. During the memorability experiment, most embodied passwords stayed within a certain range. Participants even stated that they would like to create smaller movements, but that it was not possible without feedback. Interestingly, as explained by a music conductor, small movements demand more attention and show confidence in your message. Although the smallest interfaces were regarded the safest, participants often preferred the middle-sized artefact with a height of 40 mm and a diameter of 60 mm as their embodied password. This artefact suited the dimensions of their hand, hence being the nicest to use.

Lastly, in our study, the music conductors and music conductor students associated light and free movements with complicatedness and unpredictability, which seems to be a juxtaposition. We therefore suggest that further research is needed in order to fully understand the type of movements suited for muscle memory-based passwords, and why these types of movement.

8.2 Design Elements and Future Directions

The embodied passwords used in the memorability experiment were not regarded as safe passwords, with two reasons being that they were easy to recall and felt natural to perform. Interestingly, the passwords which were seen as safe, felt complex to the participants. This could indicate that passwords need to feel complex in order to be perceived as safe. This sentiment might stem from our alphanumeric passwords, where complex rules try to force users to create safe passwords. However, in future research, we would rather pursue creating a sense of safety by adding haptic feedback. According to our research, feedback could reassure the reproducibility, add complexity, enable more complex passwords, communicate whether the password has been entered correctly or whether the correct password has been entered, and inform about the strength/uniqueness of the password. Haptic feedback is invisible to others and plays into the feeling of intimacy already experienced with embodied passwords. Moreover, prior research has already given an indication that people can recall haptic passwords [4, 5] and the work of [45, 46] gives pointers of the type of haptics suitable for rotary devices.

Although the embodied passwords were not perceived as safe by all, we believe this research has found arguments which state the opposite: participants mentioned that you cannot easily share your embodied password with others, and that you cannot easily forget and replace them. Furthermore, the strategies to come up with and recall the embodied passwords were quite unique. Of course, we clustered them in this paper, but none were identical. These

elements give an indication that embodied passwords could possibly be strong passwords. Especially when the password not only looks at what is performed, but also how it is performed. The results show that each person holds, uses, and performs their password in their own unique way. We assume that by including how someone performs their password, the security can be increased. In order to achieve this, knowledge from behavioural biometrics can be used [4].

Lastly, this research was based on the idea of utilising muscle memory. Although the memorability experiment only had the duration of a week, it seems that the embodied passwords already started to become part of the participants' muscle memory. According to Paul Fitts and Michael Posner, there are three stages of muscle memory [12]. During the first stage, movements are slow, inconsistent, inefficient, and mostly controlled consciously. In the second stage, movements have become more fluid, efficient, reliable, and are (to some extend controlled) subconsciously. The last stage shows accurate, efficient, and consistent movements, which are mainly controlled subconsciously. From the interviews and notation maps, it seems that participants were experiencing the second stage: the movements had become consistent by the third session, and participants mentioned only recalling the password when they had to perform it, the easiness of recalling, and that it felt as if they had done it their entire life, indicating that it happened without much conscious effort. Although it is known that muscle memory quickly starts to take place and continues even after the practice has ended [27, 28], the exact amount of time needed to become completely unconscious depends on the difficulty of the action. Therefore, we believe a long term experiment should be conducted to explore if and when an embodied password reaches stage three. If this happens, it would imply that people can recall an embodied password even after months of not using it.

8.3 Practicality of Embodied Passwords

Since our research is one of the first studies exploring what muscle memory-based embodied passwords should look like and their interaction capabilities, we did not yet investigate practicality. However, this should be a follow-up step for future research. A first element to explore is the practicality of the password artefact itself: should it be integrated or a separate device, how can people use and carry it in their everyday lives, how does the context influence the design and interaction? Answers to these questions are needed, in order to understand and create muscle memory-based embodied passwords which we can use in our daily lives.

Next, we should explore how (the buildup of) muscle memory differs for different physical forms. In our work, we found that a cylindrical shape works well and it seems that passwords created with our device started to become part of the participants' muscle memory. However, it might be that other shapes and interactions more quickly train our muscle memory. Therefore, future studies should explore the role of shape and interaction on muscle memory.

Lastly, we created notation maps that would serve as a hint to the participants, when they forgot their embodied password (and which provided an overview to the researchers). If movement-based passwords become a real alternative, we will need a new style of reminders and verification questions, as opposed the alphanumerical currently in use. Future studies should explore how to represent and communicate password movements and how to recall or reset 'forgotten' passwords.

8.4 Limitations

This research has several limitations. For future research we should conduct similar experiments with a more varied sample of participants and with larger participant sample sizes. For the memorability experiment, more participants would certainly provide better insights into the uniqueness of the passwords and their memorability. Furthermore, especially for the memorability experiment, the results may have been influenced by the setup: participants knew they were participating in an experiment focussing on memorability, they were asked to explain their design decisions at the end of the first session, the order in which the passwords had to be entered was always the same, and participants could practise the embodied password five times with a visualisation, in order to familiarise with the prototype. All this could have influenced the memorability of the passwords. Furthermore, the password restrictions for the alphanumeric and embodied passwords were not equal. Although it seems that people are able to recall long embodied passwords, it is advised to conduct a test with equal minimum password lengths. Moreover, the limitations of the prototypes could have influenced the created passwords. Therefore, an experiment with improved prototypes should be conducted.

Lastly, we did not explore the security of the embodied passwords. During the memorability experiment, participants were concerned about the visibility of the embodied passwords. We therefore think it is important to conduct a study which explores the visibility and reproducibility of embodied passwords by onlookers, in order to explore the safety, besides the perceived safety. A similar test has been conducted by [34], which found that the success rates of replicating a password after onlooking were extremely low for both bend passwords and PINs, which is promising for the embodied passwords. Furthermore, quite commonly the strength of an alphanumeric password is measured by calculating the entropy, e.g. [29]. Something similar could be done for embodied passwords, where the length and the speed of the movement is converted to bits. Although this was outside the scope of our research, it would allow us to calculate the strength of embodied passwords and compare it to that of alphanumeric.

9 CONCLUSION

This paper describes an explorative research towards an embodied password based on muscle memory. The results of the paper indicate that embodied passwords are memorable and reproduceable for at least a week, with a decreasing average number of attempts needed to correctly enter the password. Furthermore, embodied password are quick and easy to recall, and participants created passwords which were unique to them. Besides, this research has found that the movement space of an embodied password should be around the 200 mm × 200 mm, wherein one can create movements with a quick, strong, bound, and direct effort, and the freedom to alternate with free and light. Moreover, each password context has its own perceived necessary safety, which together with the affordances of the artefact and what we are familiar with, influences how the

password is performed. Lastly, the dimensions of the artefact have an impact as well, with smaller sized artefacts being experienced as safer. However, we found that there is a trade-off between this experienced safety and the ergonomics of the artefact. Besides, the dimensions of the artefact should be balanced on three levels: with the context, the user, and within the design itself.

Our work gives motivation to further explore embodied passwords. Future research should explore the role of feedback, how to ensure that embodied passwords feel safe to use, and whether embodied passwords are actually safe. For the latter, an important step is calculating the entropy of embodied passwords, as such calculating the strength. The contribution of this research can be used for future designs of embodied passwords, other password alternatives, or objects that could to be perceived as safe.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (12 1999), 40–46. https://doi.org/10.1145/322796.322806

[2] Jason Alexander, Anne Roudaut, Jürgen Steimle, Kasper Hornbæk, Miguel Bruns Alonso, Sean Follmer, and Timothy Merritt. 2018. Grand challenges in Shape-changing interface research. In *Conference on Human Factors in Computing Systems - Proceedings*, Vol. 2018-April. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173873

[3] Bander AlFayyadh, Per Thorsheim, Audun Jøsang, and Henning Klevjer. 2012. Improving Usability of Password Management with Standardized Password Policies. *7eme Conférence sur la …* 4 (2012), 48 – 42. https://www.researchgate.net/publication/262802201_Improving_Usability_of_Password_Management_with_Standardized_Password_Policieshttp://folk.uio.no/josang/papers/ATJK2012-SARSSI.pdf

[4] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2010. The secure haptic keypad. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*. ACM Press, New York, New York, USA, 1089. https://doi.org/10.1145/1753326.1753488

[5] Andrea Bianchi, Ian Oakley, Jong Keun Lee, and Dong Soo Kwon. 2010. The haptic wheel. In *Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems - CHI EA '10*. ACM Press, New York, New York, USA, 3625. https://doi.org/10.1145/1753846.1754029

[6] Bourns and Inc. 2019. EAW-Absolute Contacting Encoder (ACE ™). , 6 pages. https://www.bourns.com/docs/product-datasheets/ace.pdf

[7] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (1 2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[8] V. Chislett and A. Chapman. 2005. VAK Learning Styles Self-Assessment Questionnaire. https://www.businessballs.com/self-awareness/vak-learning-styles/

[9] Sangeeta Dey and A. Kapoor. 2015. Sex determination from hand dimensions for forensic identification. *International Journal of Research in Medical Sciences* 3, June, No 6 (2015), 1466–1472. https://doi.org/10.18203/2320-6012.ijrms20150169

[10] Paul Dourish. 2001. *Where the Action Is The Foundations of Embodied Interaction*. The MIT Press, Cambridge, MA. 248 pages. https://mitpress.mit.edu/books/where-action

[11] Kenneth P. Fishkin, Anuj Gujar, Beverly L. Harrison, Thomas P. Moran, and Roy Want. 2000. Embodied user interfaces for really direct manipulation. *Commun. ACM* 43, 9 (9 2000), 74–80. https://doi.org/10.1145/348941.348998

[12] Paul Fitts and Michael Posner. 1967. *Human performance*. Brooks/Cole Pub. Co., Belmont Calif. 162 pages.

[13] Maiken Hillerup Fogtmann, Jonas Fritsch, and Karen Johanne Kortbek. 2008. Kinesthetic interaction. In *Proceedings of the 20th Australasian Conference on Computer-Human Interaction Designing for Habitus and Habitat - OZCHI '08*. ACM Press, New York, New York, USA, 89. https://doi.org/10.1145/1517744.1517770

[14] Sondra Fraleigh and Maxine Sheets-Johnstone. 2002. The Primacy of Movement. *Dance Research Journal* 34, 1 (2002), 119. https://doi.org/10.2307/1478145

[15] William W. Gaver. 1991. Technology affordances. In *Proceedings of the SIGCHI conference on Human factors in computing systems Reaching through technology - CHI '91*. ACM Press, New York, New York, USA, 79–84. https://doi.org/10.1145/108844.108856

[16] James J. Gibson. 1979. *The Ecological Approach to Visual Perception*. Psychology Press, New York. 346 pages.

[17] Joseph Goldberg, Jennifer Hagman, and Vibha Sazawal. 2002. Doodling our way to better authentication. In *CHI '02 extended abstracts on Human factors in computer systems - CHI '02*. ACM Press, New York, New York, USA, 868. https://doi.org/10.1145/506621.506639

[18] Paul A Grassi, James L Fenton, Elaine M Newton, Ray A Perlner, Andrew R Regenscheid, William E Burr, Justin P Richer, Naomi B Lefkovitz, Jamie M Danker, Yee-Yin Choong, Kristen K Greene, and Mary F Theofanos. 2017. *Digital identity guidelines: authentication and lifecycle management*. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-63b

[19] Rex Hartson. 2003. Cognitive, physical, sensory, and functional affordances in interaction design. *Behaviour & Information Technology* 22, 5 (9 2003), 315–338. https://doi.org/10.1080/01449290310001592587

[20] Marc Hassenzahl, Michael Burmester, and Franz Koller. 2003. AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In *Mensch & Computer*. J.Ziegler & G. Szwillus (Eds.), Stuttgart, 187–196. https://doi.org/10.1007/978-3-322-80058-9{_}19

[21] Kristina Höök. 2018. *Designing with the Body - Somaesthetic Interaction Design*. The MIT Press, Cambridge, MA. 272 pages. https://mitpress.mit.edu/books/designing-body

[22] Eva Hornecker and Jacob Buur. 2006. Getting a grip on tangible interaction. In *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06*. ACM Press, New York, New York, USA, 437. https://doi.org/10.1145/1124772.1124838

[23] Philip G. Inglesant and Martina Angela Sasse. 2010. The true cost of unusable password policies. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*. ACM Press, New York, New York, USA, 383. https://doi.org/10.1145/1753326.1753384

[24] Hiroshi Ishii, Dávid Lakatos, Leonardo Bonanni, and Jean-Baptiste Labrune. 2012. Radical atoms. *Interactions* 19, 1 (1 2012), 38–51. https://doi.org/10.1145/2065327.2065337

[25] Anil K. Jain, Ruud Bolle, and Sharath Pankanti. 1999. *Biometrics: Personal Identification in Networked Security*. Kluwer Academic Publishers, Norwell. 411 pages. https://doi.org/10.1007/978-0-387-32659-7

[26] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. 1999. The Design and Analysis of Graphical Passwords. In *Proceedings of the 8th USENIX Security Symposium*. The USENIX Association, Washington, D.C., 1. http://arxiv.org/abs/2009.01282

[27] Avi Karni, Gundela Meyer, Christine Rey-Hipolito, Peter Jezzard, Michelle M. Adams, Robert Turner, and Leslie G. Ungerleider. 1998. The acquisition of skilled motor performance: Fast and slow experience-driven changes in primary motor cortex. *Proceedings of the National Academy of Sciences* 95, 3 (2 1998), 861–868. https://doi.org/10.1073/pnas.95.3.861

[28] Sungshin Kim, Kenji Ogawa, Jinchi Lv, Nicolas Schweighofer, and Hiroshi Imamizu. 2015. Neural Substrates Related to Motor Memory with Multiple Timescales in Sensorimotor Adaptation. *PLOS Biology* 13, 12 (12 2015), e1002312. https://doi.org/10.1371/journal.pbio.1002312

[29] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. ACM Press, New York, New York, USA, 2595. https://doi.org/10.1145/1978942.1979321

[30] John W. Krakauer and Reza Shadmehr. 2006. Consolidation of motor memory. *Trends in Neurosciences* 29, 1 (1 2006), 58–64. https://doi.org/10.1016/j.tins.2005.10.003

[31] Pierre Lévy and Bart Hengeveld. 2016. What matters for ritual visualization: towards a design tool for the description and the composition of rituals.. In *Proceedings of Kansei Engineering and Emotion Research International Conference 2016*. Japan Society of Kansei Engineering, University of Leeds, 14.

[32] Lian Loke and Toni Robertson. 2013. Moving and making strange. *ACM Transactions on Computer-Human Interaction* 20, 1 (3 2013), 1–25. https://doi.org/10.1145/2442106.2442113

[33] Yiqin Lu, Chun Yu, Xin Yi, Yuanchun Shi, and Shengdong Zhao. 2017. BlindType. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 2 (6 2017), 1–24. https://doi.org/10.1145/3090083

[34] Sana Maqsood. 2014. Shoulder surfing susceptibility of bend passwords. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*. ACM, New York, NY, USA, 915–920. https://doi.org/10.1145/2559206.2579411

[35] Sana Maqsood, Sonia Chiasson, and Audrey Girouard. 2016. Bend Passwords: using gestures to authenticate on flexible devices. *Personal and Ubiquitous Computing* 20, 4 (8 2016), 573–600. https://doi.org/10.1007/s00779-016-0928-6

[36] Wendy Moncur and Grégory Leplâtre. 2007. Pictures at the ATM. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '07*. ACM Press, New York, New York, USA, 887–894. https://doi.org/10.1145/1240624.1240758

[37] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. 2012. Leveraging motor learning for a tangible password system. In *Proceedings of the 2012 ACM annual conference extended abstracts on Human Factors in Computing Systems Extended Abstracts - CHI EA '12*. ACM Press, New York, New York, USA, 2597. https://doi.org/10.1145/2212776.2223842

[38] Salil Prabhakar, Sharath Pankanti, and Anil K. Jain. 2003. Biometric recognition: Security and privacy concerns. https://doi.org/10.1109/MSECP.2003.1193209

[39] Philip R. Ross and Stephan A.G. Wensveen. 2010. Designing behavior in interaction: Using aesthetic experience as a mechanism for design. *International Journal of Design* 4, 2 (2010), 3–13.

[40] Martina Angela Sasse, Sacha Brostoff, and D. Weirich. 2001. Transforming the 'weakest link' - A human/computer interaction approach to usable and effective security. *BT Technology Journal* 19, 3 (7 2001), 122–131. https://doi.org/10.1023/A:1011902718709

[41] Reza Shadmehr and Thomas Brashers-Krug. 1997. Functional Stages in the Formation of Human Long-Term Motor Memory. *The Journal of Neuroscience* 17, 1 (1 1997), 409–419. https://doi.org/10.1523/JNEUROSCI.17-01-00409.1997

[42] Orit Shaer. 2009. Tangible User Interfaces: Past, Present, and Future Directions. *Foundations and Trends® in Human–Computer Interaction* 3, 1-2 (2009), 1–137. https://doi.org/10.1561/1100000026

[43] Elizabeth Stobert. 2010. Usability and strength in click-based graphical passwords. In *Proceedings of the 28th of the international conference extended abstracts on Human factors in computing systems - CHI EA '10*. ACM Press, New York, New York, USA, 4303. https://doi.org/10.1145/1753846.1754144

[44] David Sweatt. 2010. *Mechanisms of Memory*. Elsevier, London, UK. 1–23 pages. https://doi.org/10.1016/C2009-0-03605-8

[45] Anke van Oosterhout and Eve Hoggan. 2020. Reshaping Interaction with Rotary Knobs. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. ACM, New York, NY, USA, 1973–1982. https://doi.org/10.1145/3357236.3395536

[46] Anke van Oosterhout, Majken Kirkegård Rasmussen, Eve Hoggan, and Miguel Bruns. 2018. Knobology 2.0. In *The 31st Annual ACM Symposium on User Interface Software and Technology Adjunct Proceedings*. ACM, New York, NY, USA, 197–199. https://doi.org/10.1145/3266037.3271649

[47] David Watson, Lee Anna Clark, and Auke Tellegen. 1988. Development and Validation of Brief Measures of Positive and Negative Affect: The PANAS Scales. *Journal of Personality and Social Psychology* 54, 6 (1988), 1063–1070. https://doi.org/10.1037/0022-3514.54.6.1063

[48] Stephan A.G. Wensveen. 2005. *A tangibility approach to affective interaction*. Ph.D. Dissertation. Technische Universiteit Delft.

[49] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies* 63, 1-2 (7 2005), 102–127. https://doi.org/10.1016/j.ijhcs.2005.04.010

[50] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. 2007. Research through design as a method for interaction design research in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '07*. ACM Press, New York, New York, USA, 493–502. https://doi.org/10.1145/1240624.1240704